BERICHT

McAfee
Together is power.

Der große Datenklau

Studie zur Datenexfiltration: Akteure, Taktiken und Erkennung

Inhaltsverzeichnis

Der große Datenklau

Studie zur Datenexfiltration: Akteure, Taktiken und Erkennung

Einleitung

Sicherheitsexperten haben in den letzten Jahren so einiges zu Gesicht bekommen. Diejenigen Befragten, die bereits eine Datenkompromittierung festgestellt haben, berichteten jeweils von durchschnittlich sechs erheblichen Sicherheitsverstößen. Bei 68 % dieser Zwischenfälle wurden Daten aus dem Netzwerk exfiltriert, die so wichtig waren, dass der Vorfall öffentlich gemacht werden musste oder ein finanzieller Schaden für das Unternehmen entstand – bei 70 % der Zwischenfälle in kleineren Unternehmen und 61 % in Großunternehmen. Die durchschnittliche Anzahl von Kompromittierungen war in Unternehmen im Asien-Pazifik-Raum am höchsten und bei Unternehmen in Großbritannien und den USA am niedrigsten. Mehr als 10 % der Unternehmen im Asien-Pazifik-Raum meldeten mehr als 20 Kompromittierungen. Im Vergleich dazu gaben in Nordamerika nur 1 % und in Großbritannien 4 % der Unternehmen eine so hohe Zahl an Kompromittierungen an.

Die meisten Sicherheitsstudien und -statistiken konzentrieren sich auf die Infiltration, also darauf, wie Angreifer Schutzmechanismen überwinden und in das Netzwerk eindringen. Dieser Teil des Angriffs ist sichtbarer, da Computer kompromittiert und Ereignisse und Alarme im Sicherheitskontrollzentrum ausgelöst werden. Bis jetzt gab es nur wenige Informationen zum weniger sichtbaren Vorgang der Datenexfiltration, also dazu, wie Angreifer Daten entwenden. Ob Sie es nun sehen können oder nicht: Datenexfiltration stellt für die meisten Unternehmen ein ernstzunehmendes Risiko dar. In diesem Bericht geht es um die Probleme und Herausforderungen, mit denen Unternehmen (1.000 bis 5.000 Mitarbeiter) und Großunternehmen (mehr als 5.000 Mitarbeiter) in Australien, Großbritannien, Indien, Kanada, Neuseeland, Singapur und den USA konfrontiert werden.

Aufbauend auf der letzten Studie von McAfee zu **den fünf häufigsten Angriffsmethoden**, **der Verbesserung der Angriffserkennung und Reaktion auf Zwischenfälle** und **dem Schutz kritischer Infrastrukturen** haben wir eine neue Studie durchgeführt, um Datenexfiltration besser verstehen zu können. Wir sprachen mit IT- und Sicherheitsexperten, die über Entscheidungsbefugnisse verfügen und für 1.155 Unternehmen weltweit tätig sind, und haben 522 befragt, die bereits mindestens eine ernsthafte Datenkompromittierung in ihrem jetzigen oder vorherigen Job festgestellt haben. Wir befragten sie zu ihren größten Sorgen, Kompromittierungen und Exfiltrationen, Bedrohungen von außen und innen, Unterschieden bei der Exfiltration zwischen herkömmlichen Netzwerken und Cloud-Anwendungen sowie den dabei verwendeten Tools

und Vorgehensweisen zur Erkennung und Verhinderung von Datenexfiltration. Wie bereits frühere Studien gezeigt haben, waren der Schutz und die Vertraulichkeit von Kunden- sowie Mitarbeiterdaten das größte Problem, und unzureichende Sicherheitsmaßnahmen stellten angesichts der immer raffinierteren Angriffe die größte Herausforderung dar. Interessanterweise waren Bedrohungen durch Insider, zum Beispiel durch verärgerte Mitarbeiter, das zweitgrößte Problem bei den Befragten aus dem Asien-Pazifik-Raum, während sie insgesamt nur an sechster Stelle lagen.

Ergebnisse

- Interne Akteure waren für 43 % der Datenverluste verantwortlich, von denen jeweils die Hälfte absichtlich bzw. versehentlich erfolgte.
- Der Diebstahl physischer Medien ist nach wie vor ziemlich weit verbreitet und trat bei 40 % der Exfiltrationen auf.
- 64 % der Sicherheitsexperten waren der Ansicht, dass Technologien zum Schutz vor Datenkompromittierung (Data Loss Prevention, DLP) die vorgekommenen Datenexfiltrationen hätten verhindern können.
- Bei 25 % der Datenexfiltrationen wurden Dateiübertragungs- oder Tunneling-Protokolle (z. B. FTP oder SCP) verwendet.
- 32 % der exfiltrierten Daten waren verschlüsselt.
- Microsoft Office-Dokumente waren bei gestohlenen Daten das am häufigsten verwendete Format (25 %).
- Persönliche Informationen von Kunden sowie Mitarbeitern waren das häufigste und beliebteste Ziel (62 %), da der Wert privater Daten den von Kreditkarten mittlerweile übersteigt.
- Die damit verbundenen Cloud-basierten Implementierungen haben die Angst vor noch mehr Sicherheitsverstößen erhöht, obwohl es keine Anzeichen dafür gab, dass mit Cloud-Anwendungen ein höheres Risiko einhergeht.
- Sicherheitsexperten, die bereits seit mindestens fünf Jahren bei ihrem derzeitigen Arbeitgeber tätig sind, haben die Sicherheitsmaßnahmen gestärkt und das Risiko schwerwiegender Datenexfiltrationen gesenkt.
- Die Befragten, die DLP-Technologien verwenden, standen in enger Verbindung zu internen Teams, die sich um die Erkennung und Verhinderung von Datendiebstählen kümmern.

Die Täter: Vergleich zwischen externen und internen Akteuren

Unsere Studie zeigt, dass interne Akteure für mehr als 40 % der von den Befragten festgestellten schwerwiegenden Datenkompromittierungen verantwortlich waren, der Anteil interner Akteure lag bei knapp unter 60 %.

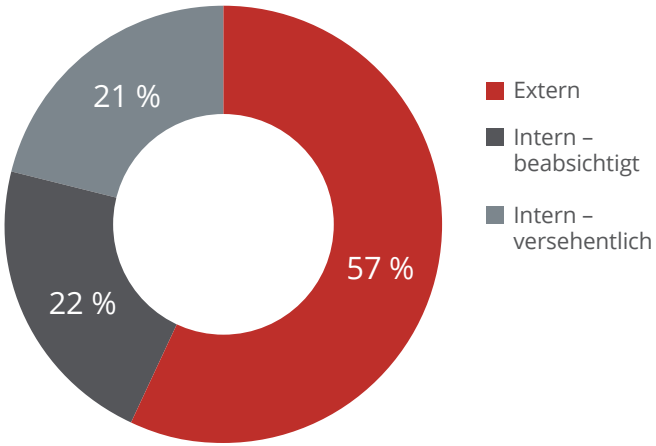

Abbildung 1. Die in Datenkompromittierungen verwickelten Akteure

Zu den internen Akteuren gehören Mitarbeiter, Auftragnehmer und externe Lieferanten, wobei das Verhältnis zwischen Mitarbeitern/Auftragnehmern und Lieferanten 60:40 beträgt. Wenn interne Akteure in Datenexfiltrationen verwickelt waren – ob nun absichtlich (etwas mehr als die Hälfte der Fälle) oder versehentlich –, haben sie eher physische Medien (vor allem USB-Laufwerke und Laptops) anstelle elektronischer Methoden verwendet. Mitarbeiterdaten, und zwar sowohl Identitäts- als auch Gesundheitsdaten, stellten für interne Akteure ein größeres Ziel dar als Kundendaten. Möglicherweise ist dies in der besseren Zugänglichkeit begründet. Office-Dokumente waren das häufigste Format bei den von internen Akteuren gestohlenen Daten – vermutlich weil diese Dokumente auf Geräten von Mitarbeitern gespeichert sind und viele Unternehmen nur wenige Kontrollmaßnahmen für Daten festlegen, die sich nicht mehr in einer Datenbank befinden. Fast 50 % der Datenverluste im Asien-Pazifik-Raum entfielen auf Diebstähle durch Insider, während es in Großbritannien weniger als 40 % und in Nordamerika 41 % waren.

Welche Daten werden gestohlen?

Datentypen	Interne Akteure	Externe Akteure
Kundendaten	27 %	32 %
Mitarbeiterdaten	33 %	28 %
Geistiges Eigentum	15 %	14 %
Zahlungskartendaten	11 %	15 %
Sonstige Finanzdaten	14 %	11 %

Datentypen	Nord-amerika	Groß-britannien	Asien-Pazifik-Raum
Kundendaten	31 %	32 %	34 %
Mitarbeiterdaten	32 %	25 %	27 %
Geistiges Eigentum	13 %	19 %	12 %
Zahlungskartendaten	13 %	14 %	14 %
Sonstige Finanzdaten	11 %	10 %	13 %

Welche Formate werden gestohlen?

Formate	Interne Akteure	Externe Akteure
Microsoft Office (Excel, PowerPoint, Word)	39 %	21 %
Klartext/CSV	20 %	21 %
PDF	11 %	20 %
Bilder und Videos	11 %	18 %
XML	12 %	19 %
Sonstige	7 %	1 %

Formate	Nord-amerika	Groß-britannien	Asien-Pazifik-Raum
Microsoft Office (Excel, PowerPoint, Word)	22 %	30 %	27 %
Klartext/CSV	24 %	18 %	16 %
PDF	20 %	13 %	17 %
Bilder und Videos	16 %	19 %	19 %
XML	17 %	17 %	18 %
Sonstige	1 %	3 %	3 %

Die Befragten, die hauptsächlich über Kompromittierungen durch Insider berichteten, verfügen über keine fundierten Kenntnisse zu E-Mail-Sicherheit, Web-Sicherheit und Schutz vor Datenkompromittierung (DLP). Im Vergleich zu denjenigen, die vor allem externe Angriffe festgestellt haben, setzen sie seltener entsprechende Technologien ein. Dies zeigt sich insbesondere dadurch, dass DLP als eines der zwei wichtigsten Sicherheits-Tools für das Feststellen von Datendiebstählen durch Insider genannt wurde.

Zu den externen Akteuren gehören in der Reihenfolge ihrer Bedeutung: Hacker, Malware-Entwickler, organisierte Kriminalität, Aktivisten und staatliche Geheimdienste. Organisierte Kriminalität, Aktivisten und Staaten wurden im Asien-Pazifik-Raum 30 % häufiger als externe Akteure identifiziert als in anderen Ländern. Beim Diebstahl durch externe Akteure blieben Microsoft Office-Dokumente weiterhin das häufigste Format für Exfiltrationen, lagen jedoch nur ein paar Prozentpunkte vor Klartext, CSV-Dateien oder PDF. Der Diebstahl von Bildern und Videos wurde eher von externen als von internen Akteuren begangen, möglicherweise aufgrund des Wertes von Bildern prominenter oder anderer öffentlichen Personen in kompromittierenden oder peinlichen Situationen. Wenn physische Medien beteiligt waren, hatten es externe Akteure eher auf Laptops, Mobiltelefone und Webcams abgesehen. Externe Angreifer stahlen auch eher Kunden- statt Mitarbeiterdaten und hatten mehr Interesse an Zahlungskartendaten als interne Akteure.

Angesichts der erheblichen Anzahl an Exfiltrationen durch interne Akteure (43 %) sollten Unternehmen ihre Lehre daraus ziehen. Die Überprüfung der betrieblichen Abläufe sowie Schulungsprogramme zur Auffrischung der Mitarbeiterkenntnisse können dabei helfen, die 50 % versehentlichen Datenverluste zu reduzieren. Um angemessene Maßnahmen gegen absichtliche interne Bedrohungen zu implementieren, sollten Unternehmen ihre Sicherheitstechnologien überprüfen und die vorhandenen Kontrollmaßnahmen identifizieren, mit denen die Daten vor physischer Extraktion (z. B. Diebstahl von Laptops oder Übertragung von Daten auf ein USB-Laufwerk) und digitaler Extraktion (z. B. E-Mail-Übertragung oder das Hochladen auf Cloud-Dienste) geschützt werden.

„Organisierte Kriminalität, Aktivisten und Staaten wurden im Asien-Pazifik-Raum 30 % häufiger als externe Akteure identifiziert als in anderen Ländern.“

Welche Daten werden gestohlen und wie?

Unternehmen stellen Datenverluste bei einer Vielzahl an Inhalten, Formaten und Methoden fest – von Dokumenten bis hin zu Datenbanken, die elektronisch oder physisch von internen oder externen Personen gestohlen werden. Mehr als 90 % der Sicherheitsverstöße im Asien-Pazifik-Raum haben zu einer tatsächlichen Exfiltration von Daten geführt, während es in Nordamerika 84 % und in Großbritannien 80 % waren.

60 % der gemeldeten Datenexfiltrationen erfolgten durch direkte elektronische Hilfsmittel, während bei den anderen 40 % in irgendeiner Form physische Medien involviert waren (z. B. gestohlene Laptops oder Downloads auf ein USB-Laufwerk).

Kunden- und Mitarbeiterdaten waren bei den Inhalten die zwei Top-Kategorien, darunter personenbezogene Informationen und persönliche Gesundheitsdaten. Geistiges Eigentum rangiert in der Beliebtheit der Inhaltskategorien gleich dahinter, gefolgt von Zahlungskartendaten und sonstigen Finanzdaten.

Das am häufigsten exfiltrierte Datenformat waren Microsoft Office-Dokumente, gefolgt von Klartext oder CSV-Dateien, PDFs, Bildern und Videos sowie XML.

Office-Dokumente führten die Liste in Großbritannien und in den Ländern des Asien-Pazifik-Raums an, während in Nordamerika Klartext und CSV-Dateien an die erste Stelle rückten. Dies könnte daran liegen, dass in Nordamerika bei Diebstählen vermehrt Rechenzentren und Datenbankspeicher anstelle von PCs und anderen Endgeräten ins Visier genommen wurden.

Wie werden die Daten gestohlen?

Methode zur Datenexfiltration	Interne Akteure	Externe Akteure
Physische Medien		
Laptops/Tablets	11 %	13 %
USB-Laufwerke	15 %	8 %
Mobiltelefone	3 %	6 %
Papierausdrucke	3 %	4 %
CDs/DVDs	4 %	4 %
Mikrofone/Webcams	2 %	4 %
Faxe	2 %	3 %
Elektronische Methoden		
Web-Protokolle	15 %	16 %
Dateiübertragungsprotokolle	11 %	15 %
E-Mail	10 %	10 %
Peer-to-Peer	6 %	4 %
SSH/VPN	3 %	6 %
Windows Management (WMI)	7 %	5 %
Bilder oder Videos	6 %	5 %
Routing Control-Pakete	3 %	4 %
Voice-over-IP (VoIP)	3 %	4 %
Sofortnachrichten	3 %	3 %
Desktop-Fernzugriff	2 %	3 %
Sonstige	5 %	0 %

Der vielleicht interessanteste Teil der Umfrage befasst sich damit, wie Daten gestohlen wurden. Die 40 % der mithilfe physischer Medien gestohlenen Daten betrafen hauptsächlich Laptops, Tablets oder USB-Laufwerke. Mobiltelefone waren bei 15 % der physischen Diebstähle beteiligt, was vermutlich mit der zunehmenden Akzeptanz von Bring-Your-Own-Device-Programmen zu tun hat. Ältere Typen von physischen Medien (z. B. Papierausdrucke, CDs, DVDs und Faxe) werden jedoch nach wie vor zum Extrahieren von Unternehmensdaten verwendet, sodass Sicherheitsteams diese weiterhin in ihre Planung einbinden müssen. Sogar Mikrofone und Webcams waren betroffen und für fast 10 % der physischen Diebstähle verantwortlich.

Bei den 60 % der elektronisch gestohlenen Daten waren verschiedene Web-Protokolle, Dateiübertragungs- und Tunneling-Protokolle beteiligt. Bei 5 bis 10 % der Fälle wurde jedoch eine Vielzahl anderer Protokolle und Methoden eingesetzt, zum Beispiel Peer-to-Peer, Secure Shell, Routing Control-Pakete, Windows Management Instrumentation, Sofortnachrichten, VoIP und das Verbergen der Daten in Bildern oder Videos. Darüber hinaus tarnen die Angreifer die gestohlenen Daten mittels Verschlüsselung, Komprimierung, Verschleierung, Chunking und Steganografie, um sie vor den Sicherheitsmechanismen abzuschirmen.

Diese Bandbreite an Protokollen und Verschleierungsmethoden veranschaulicht die zunehmende Raffinesse der Cyber-Angriffe und zeigt, warum Peripherie- und Endgeräteschutz allein nicht genügen, um Datenexfiltrationen durch Bedrohungen von inner- und außerhalb des Unternehmens zu verhindern.

Exfiltration: Vergleich zwischen herkömmlichen und Cloud-Netzwerken

Viele Technologien und Anwendungen werden in die Cloud verlagert. Rund 60 % der Befragten setzen offiziell Cloud-basierte Anwendungen ein, wobei der Prozentsatz im Hinblick auf die Nutzung von Cloud-Anwendungen bei Großunternehmen etwas höher ist als bei anderen Unternehmen. In Nordamerika tendierten die Cloud-basierten Implementierungen noch deutlich mehr in Richtung der Großunternehmen, von denen 75 % Cloud-Anwendungen nutzen, verglichen mit 56 % bei anderen Unternehmen, während in Großbritannien fast genau das Gegenteil der Fall war. In Großbritannien gab es auch insgesamt mehr Cloud-basierte Implementierungen, und zwar nahezu 70 %. Weniger als die Hälfte der Befragten von Unternehmen und Großunternehmen aus dem Asien-Pazifik-Raum nutzt Cloud-Anwendungen, was vermutlich auf die Bandbreiten- und Latenzbeschränkungen oder die größere Sorge im Hinblick auf eine Kompromittierung von Cloud-Diensten zurückzuführen ist. Insbesondere Professional Services-Anbieter und Produktionsunternehmen gaben eine intensivere Nutzung von Cloud-Anwendungen als die anderen vertretenen Branchen an.

Unternehmen, in denen Cloud-Anwendungen implementiert sind, waren häufiger mit einer Vielzahl an Sicherheitstechnologien vertraut und haben wahrscheinlich bereits die volle Bandbreite an Tools im Einsatz. Sie verwendeten Cloud-Anwendungen zudem mit einem stärkeren Bewusstsein für Bedrohungen: Im Durchschnitt waren die Befragten in solchen Unternehmen der Meinung, dass schwerwiegende Kompromittierungen in den nächsten zwei Jahren tendenziell zunehmen werden. In Anbetracht der Tatsache, dass nahezu alle Befragten bereits Cloud-Anwendungen implementiert haben oder dies in den nächsten 12 Monaten vorhaben, scheinen die Vorteile von Clouds die Risiken für die meisten Unternehmen zu überwiegen.

Bei Diebstählen von Unternehmensdaten waren bei fast zwei Drittel der Kompromittierungen herkömmliche Unternehmensnetzwerke involviert – das andere Drittel entfiel auf Cloud-Einbrüche. Während im Asien-Pazifik-Raum weniger Cloud-basierte Implementierungen festgestellt wurden, gab es einen höheren Prozentsatz an Cloud-basierten Diebstählen. In Nordamerika und Großbritannien gab es mehr Diebstähle in herkömmlichen Netzwerken, jedoch mehr Cloud-basierte Implementierungen. Somit war bei dieser Studie kein statistischer Zusammenhang zwischen der Anzahl Cloud-basierter Implementierungen und dem Risiko eines Sicherheitsverstoßes festzustellen. Vielmehr geht es möglicherweise darum, dass die Diebe dahin gehen, wo es wirklich etwas zu holen gibt.

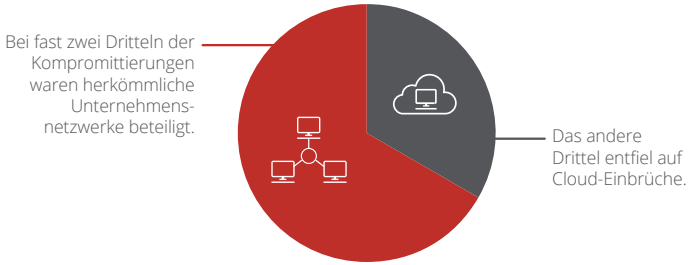

Abbildung 2. Vergleich zwischen Einbrüchen in Clouds und in herkömmlichen Netzwerken

Bei Unternehmen mit Datenkompromittierungen in einem herkömmlichen Netzwerk blieb die Anzahl entsprechender Zwischenfälle insgesamt tendenziell etwas geringer, was vermutlich auf deren Fähigkeit verweist, direkt dagegen vorzugehen und Schwachstellen zu beheben. Kompromittierungen in der Cloud führten hingegen eher zu einer tatsächlichen Datenexfiltration. Bezogen auf den Inhalt liegt der Anteil bei den Kompromittierungen in herkömmlichen und in Cloud-Netzwerken in etwa gleich: Personenbezogene Daten von Kunden waren zu 22 % in herkömmlichen Netzwerken und zu 20 % in Cloud-Netzwerken von Diebstahl betroffen. Persönliche Informationen von Mitarbeitern wurden zu 19 % bei Zwischenfällen in herkömmlichen Netzwerken und zu 18 % in der Cloud entwendet. Zahlungskartendaten wurden bei jeweils 14 % der Kompromittierungen in Cloud- und herkömmlichen Netzwerken gestohlen. Diese Ergebnisse zeigen, dass Unternehmen, die in Cloud-Netzwerke investiert haben oder diese erweitern möchten, eine Bewertung der im Rechenzentrum oder vom Datendienst verwendeten Sicherheitskontrollen vornehmen sollten, wie es üblicherweise auch für das Unternehmensnetzwerk erfolgt.

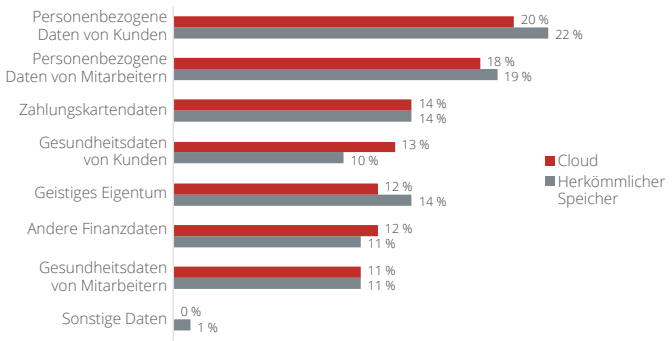

Abbildung 3. Vergleich der Typen von Daten, die in Cloud- und herkömmlichen Netzwerken anvisiert werden

Weiterbildung und Erfahrung zählen

Weiterbildung und Erfahrung spielen bei der Erkennung und Verhinderung von Datenexfiltrationen eine wichtige Rolle. Die Umfrageteilnehmer bestanden fast zu gleichen Teilen aus Experten, die mehr als fünf Jahre bei ihrem derzeitigen Arbeitgeber tätig sind, und solchen, die weniger als fünf Jahre dort tätig sind.

Experten mit mehr als fünf Jahren Erfahrung bei ihrem derzeitigen Arbeitgeber waren häufiger mit einer Vielzahl an Sicherheitstechnologien vertraut und haben diese bereits im Einsatz, um für tiefgreifende Sicherheitsmaßnahmen zu sorgen. Insgesamt war die Implementierung von Sicherheitstechnologien in Großbritannien stärker ausgeprägt als in jedem anderen Land.

Im Vergleich zu denjenigen, die noch nicht so lange bei ihrem derzeitigen Arbeitgeber tätig sind, nutzen erfahrene Experten eine größere Bandbreite an Quellen zur Informationssammlung sowie zur Weiterbildung. Zu den Quellen gehören insbesondere externe Berater wie Forensikunternehmen, Cyber-Infrastrukturanbieter und Unternehmen, die sich auf Identitätsdiebstahl und Kreditüberwachung konzentrieren. Sie waren zudem häufiger vorbereitet – mit Risikobewertungen und Auswirkungsanalysen für gefährdete Bereiche, Programmen zur Steigerung des Sicherheitsbewusstseins im Hinblick auf Privatsphäre und Datenschutz sowie Reaktionsplänen für Datenkompromittierungen. Ob es nun am größeren Selbstvertrauen, der höheren Komfortstufe oder der längeren Beschäftigungsdauer liegt: Es ist in jedem Fall ein überzeugendes Argument für die Bindung der Sicherheitsexperten an das Unternehmen und für Investitionen in ihre berufliche Weiterentwicklung. Durch Erfahrung wird auch ein höheres Maß an Vertrautheit mit den geschäftlichen Abläufen, den Architekturen, der Speicherung, Verarbeitung sowie den Anwendungen aufgebaut, und sie hilft dabei, die Effizienz von Sicherheitslösungen zu erhöhen. Mit anderen Wort: Ein häufiger Personalwechsel innerhalb des Sicherheitsteams könnte das Risiko einer weiteren Datenkompromittierung erhöhen.

Ressourcen zur Verhinderung von Datenkompromittierungen

In welchen der folgenden Quellen informieren Sie sich über Möglichkeiten zur Verhinderung und/oder Bewältigung einer Datenkompromittierung?	Mindestens fünf Jahre beim derzeitigen Arbeitgeber	Weniger als fünf Jahre beim derzeitigen Arbeitgeber
Publikationen und Websites zu Datenschutz und Sicherheit	72 %	66 %
Verbände und Konferenzen zu Datenschutz und Sicherheit	67 %	62 %
Sicherheitstechnologie/ Software-Anbieter	66 %	60 %
Informationen von Forensikunternehmen, Cyber-Infrastrukturanbietern und Unternehmen mit dem Schwerpunkt Identitätsdiebstahl/ Kreditüberwachung	53 %	40 %
Geschäftspublikationen und Fernsehsendungen	20 %	10 %

Sicherheitsteams können die Sicherheitslage ihres Unternehmens verbessern, indem sie von Kollegen mit mehr Erfahrung lernen und folgende Schritte durchführen:

- Investitionen in Sicherheitsschulungen für die Mitarbeiter und in die Entwicklung eines Sicherheitskontrollzentrums.
- Erhöhung der Häufigkeit der Netzwerküberwachung auf ungewöhnlichen oder anormalen Datenverkehr von wöchentlich oder monatlich auf mindestens täglich oder kontinuierlich. Fast 70 % der Experten mit mindestens fünf Jahren Erfahrung überwachen das Netzwerk des Unternehmens mindestens täglich – bei denjenigen mit weniger als fünf Jahre Erfahrung liegt der Anteil bei 57 %.
- Erweiterung ihrer Kenntnisse über hilfreiche Maßnahmen durch Lesen von mehr Publikationen zu Datenschutz und Sicherheit, Teilnahme an Verbandstreffen und Konferenzen, Einholen von Informationen von externen Experten und Beachtung von branchenbezogenen Geschäftspublikationen.
- Erstellung von Risikobewertungen und Notfallreaktionsplänen.
- Fokussierung auf grundlegende Sicherheitspraktiken wie Mitarbeiterschulungen und Bewusstseinsbildung. Diejenigen mit mehr Erfahrung erkennen, dass unzureichende Sicherheitspraktiken von Nutzern nach wie vor die mit Abstand größte Bedrohung für Unternehmen darstellen.

Verwendete Technologien zur Erkennung und Verhinderung

Ein einzelnes Tool oder eine Technologie allein kann nicht alle Datensicherheitsprobleme lösen. Dennoch hätten DLP-Technologien die vorgekommenen Datenexfiltrationen nach Ansicht von 70 % der Befragten verhindern können. Diese Meinung wurde insbesondere bei den Unternehmen vertreten, die diese Technologien eher nicht installiert hatten. Zusammen mit DLP machten Systeme zur Erkennung und Verhinderung von Eindringungsversuchen sowie Firewalls der nächsten Generation den größten Anteil bei der Erkennung und Verhinderung von Datenkompromittierungen aus. Unternehmen, die ihr Netzwerk im Hinblick auf ungewöhnliches oder anormales Verhalten kontinuierlich überwachen, haben häufiger Datenkompromittierungen mithilfe interner Ressourcen entdeckt und mussten keine Exfiltrationen feststellen.

„… fast 70 % der Befragten waren der Ansicht, dass Technologien zum Schutz vor Datenkompromittierung (DLP) die vorgekommenen Datenexfiltrationen hätten verhindern können.“

Die kontinuierliche Netzwerküberwachung und die DLP-Technologie standen in deutlichem Zusammenhang mit einer verbesserten Sicherheitslage und Erkennung von Kompromittierungen. Diejenigen mit implementierten DLP-Technologien waren stärker mit Sicherheitstechnologien vertraut, hatten diese eher implementiert und nutzten Weiterbildungen sowie Sicherheitsinformationen intensiver. Zudem lag bei ihnen die Wahrscheinlichkeit, dass ihr internes Sicherheitsteam Datenkompromittierungen entdeckt, 15 % höher. Leider wurde DLP bei vielen Unternehmen erst dann implementiert oder die Implementierung geplant, nachdem eine schwerwiegende Datenkompromittierung festgestellt wurde, die öffentlich bekanntgegeben werden musste. Oftmals befand sich DLP im Überwachungsmodus, ohne Maßnahmen auszulösen. Bei den kleineren Unternehmen nutzt der geringste Anteil der Umfrageteilnehmer derzeit DLP, während fast 80 % der Großunternehmen in Nordamerika DLP derzeit installiert haben.

Die Erkennungen schwerwiegender Datenkompromittierungen gelang internen Sicherheitsteams in Großbritannien in knapp mehr als der Hälfte (55 %) der Fälle, während es in Nordamerika etwas weniger als der Hälfte (48 %) und im Asien-Pazifik-Raum sogar noch weniger (39 %) internen Teams gelang. Der Rest wurde durch externe Vertreter, wie gutwillige Hacker (White Hats), Kreditkartenunternehmen und Strafverfolgungsbehörden, aufgedeckt. Die Entdeckung von Kompromittierungen durch externe Akteure teilte sich fast 50:50 zwischen internen Sicherheitsmitarbeitern und externen Vertretern auf, während mehr als zwei Drittel der Diebstähle durch Insider von internen Sicherheitsteams entdeckt wurden. Erstaunlicherweise wurden bei mittelgroßen Unternehmen (2.500 bis 5.000 Mitarbeiter) Kompromittierungen am häufigsten von externen Vertretern entdeckt, möglicherweise aufgrund der zunehmenden Ängste und Budgetbelastungen angesichts der Weiterentwicklung der IT- und Sicherheitsunternehmen.

Wenn Sicherheitszwischenfälle durch das interne Sicherheitsteam entdeckt wurden, musste das Unternehmen eher keinen tatsächlichen Datenverlust oder -diebstahl befürchten. Dies ist nicht sonderlich überraschend, da externe Vertreter eine Exfiltration wirklich erst dann entdecken können, wenn Daten bereits veröffentlicht wurden oder durchgesickert sind. Wenn Kompromittierungen durch das interne Sicherheitsteam erkannt wurden, berichteten Sicherheitsexperten von durchschnittlich zwei Zwischenfällen bei ihrem derzeitigen Arbeitgeber, während es bei Erkennungen durch zumeist externe Einrichtungen im Durchschnitt fünf Zwischenfälle waren. Intern entdeckte Zwischenfälle führen zudem weniger häufig (in 70 % der Fälle) zu einer tatsächlichen Datenexfiltration – bei extern festgestellten Zwischenfällen liegt die Wahrscheinlichkeit bei 92 %. Interne Teams haben darüber hinaus unterschiedliche Dinge entdeckt. Beispielsweise haben sie häufiger Hacker, undichte Stellen bei Mitarbeitern sowie den Diebstahl von Laptops oder USB-Laufwerken aufgedeckt. Externe Gruppen entdecken eher Angriffe durch organisierte Kriminalität, Aktivisten, staatliche Geheimdienste, gestohlene Bilder und Videos, undichte Stellen bei externen Lieferanten sowie Diebstähle, die mithilfe sonstiger physischen Medien wie Mobiltelefone, Ausdrucke, CDs/DVDs und Faxe erfolgten.

Arten von intern und extern entdeckten Kompromittierungen im Vergleich

Interne Teams	Externe Gruppen
▪ Hacker	▪ Organisierte Kriminalität oder Aktivisten
▪ Undichte Stellen bei Mitarbeitern	▪ Gestohlene Bilder
▪ Diebstahl von Laptops oder USB-Laufwerken	▪ Gestohlene Videos
	▪ Undichte Stellen bei externen Lieferanten
	▪ Diebstähle mithilfe physischer Medien (z. B. Mobiltelefone)

Insbesondere Sicherheitsexperten in Unternehmen mit einem höheren Anteil an Kompromittierungen durch externe Akteure oder extern entdeckten Kompromittierungen sahen häufiger zahlreiche Ursachen für ihre Datenverluste, z. B. unzureichende Sicherheitsschulungen, fehlende Aktualisierung der Sicherheits-Patches, Handlungen von Mitarbeitern sowie unzureichende finanzielle Unterstützung seitens der Geschäftsleitung. Bei den mittleren Unternehmen wurde am häufigsten eine unzureichende finanzielle Unterstützung als Hauptursache genannt. Diejenigen mit häufigeren Exfiltrationen durch Insider oder internen Aufdeckungen waren mehr auf gezielte Phishing-Angriffe sowie unzureichende Sicherheitsschulungen und fehlendes Problembewusstsein als Hauptursachen fokussiert.

Fazit

Der Sicherheitsmarkt konzentriert sich im Allgemeinen mehr auf die Verhinderung von Eindringungen in das Netzwerk als auf die Erkennung sowie Blockierung von Datenexfiltrationen. Die Verhinderung von Infektionen ist zwar nach wie vor wichtig, doch die Sicherheitstechnologien müssen auch nach Kompromittierungsindikatoren suchen sowie wertvolle Daten vor Exfiltration schützen. Auf Sicherheitsverstöße reagierten die meisten Unternehmen mit dem Kauf weiterer Sicherheitsprodukte und verstärkten Investitionen in Sicherheitsschulungen für Mitarbeiter. Unternehmen im Asien-Pazifik-Raum, die insgesamt eine höhere Anzahl an Kompromittierungen und ein entsprechend höheres Maß an Sicherheitsbedenken angaben, nahmen diese Schritte häufiger vor und investierten zudem in ihre Sicherheitskontrollzentren sowie in die Einstellung weiterer Mitarbeiter.

Da interne Akteure für einen so hohen Prozentsatz an Datenverlusten verantwortlich sind und davon zudem zur Hälfte versehentlich erfolgt, kann einfaches dynamisches Feedback schon viel bewirken. Beispielsweise lässt sich riskantes Verhalten effektiv verringern, wenn Mitarbeiter durch Pop-up-Meldungen darüber informiert werden, dass ihre Nachricht aufgrund des sensiblen Inhalts an den Vorgesetzten und das Sicherheitskontrollzentrum weitergeleitet wird.

Physische Medien bergen weiterhin ein großes Risiko, und die zunehmende Dichte von Flash-Speichern sowie die immer höhere Speicherkapazität der Geräte erhöhen das Risikopotenzial zusätzlich. Während klassischer Peripherie- und Endgeräteschutz nur wenig Schutz bietet, können andere Technologien wie Verschlüsselung, Schutz vor Datenkompromittierung und sogar Cloud-Anwendungen dazu beitragen, dieses Risiko zu verringern.

Die wachsende Menge und Komplexität der von Unternehmen erfassten sowie gespeicherten persönlichen Daten erhöht den Wert dieser Informationen exponentiell. Für den Schutz dieser wertvollen Daten sind nicht nur die verwendeten Sicherheitstechnologien von Bedeutung. Mindestens genauso wichtig sind die Bestimmung der Daten, deren Erfassung und Speicherung gerechtfertigt ist, die Entwicklung detaillierter Datenrichtlinien sowie regelmäßige Erinnerungen an die Mitarbeiter über die Bedeutung von Datenschutz und Vertraulichkeit.

Cloud-Anwendungen und die Verarbeitung sowie Speicherung von Daten in der Cloud werden bereits von einem Großteil der Unternehmen weltweit genutzt – Tendenz steigend. Nahezu alle Befragten, die noch keine Cloud-Anwendungen implementiert hatten, planen diesen Schritt im Laufe des nächsten Jahres. Die Cloud-Nutzung sorgt für größere Angst in Bezug auf Sicherheitsverstöße. Anbieter von Sicherheitstechnologien haben dies jedoch erkannt, und bereits heute stehen Lösungen zur Verfügung, mit denen der Speicherort und die Speichermethoden für sensible Daten sowie die Zugangsrechte auf diese Daten kontrolliert werden können. Eine größere Vertrautheit mit den Sicherheitstechnologien und deren Implementierung wurden jedoch deutlich mit einem besseren Cloud-Erlebnis in Verbindung gebracht.

Was können Sie tun, um Datenkompromittierungen zu verhindern? Bemühen Sie sich, Ihre Sicherheitsexperten für lange Zeit zu binden. Ob es nun der höhere Komfort oder das Lernen aus den eigenen Fehlern ist: Experten mit einer längeren Beschäftigungsdauer bei ihrem derzeitigen Arbeitgeber haben vielfältigere sowie effektivere Sicherheitsmaßnahmen implementiert, und sie verfügen über umfassendere Pläne und Bewertungen, die auf einer größeren Bandbreite an Weiterbildungs- sowie Informationsquellen basieren.

Falls Sie noch keine DLP-Technologien und Systeme zur Erkennung sowie Verhinderung von Eindringungsversuchen installiert haben, sollten Sie sich über deren Vorteile informieren, da sie deutlich zur Erkennung und Verhinderung von Datenexfiltration beitragen. Wenn sie bereits installiert sind, stellen Sie sicher, dass sie richtig konfiguriert sind und aktiv zu Ihrer Sicherheit beitragen und nicht standardmäßig in einem passiven Beobachtungsmodus nutzlos vor sich hin vegetieren. Durch diese Kombination aus Sicherheits-Tools, Reaktionsplänen, Schulungen zur Steigerung des Sicherheitsbewusstseins sowie Weiterbildung ist Ihr Unternehmen besser geschützt, und das Risiko von Datenverlusten wird gesenkt.

Weitere Informationen

Weitere Informationen zum Schutz vor Daten-kompromittierung finden Sie unter **www.mcafee.com/de/products/total-protection-for-data-loss-prevention.aspx**.
Weitere Informationen zur Erkennung und Verhinderung von Eindringungsversuchen finden Sie unter **www.mcafee.com/de/products/network-security-platform.aspx**.

Informationen zu McAfee

McAfee ist eines der weltweit führenden unabhängigen Cyber-Sicherheitsunternehmen. Inspiriert durch die Stärke, die aus Zusammenarbeit resultiert, entwickelt McAfee Lösungen für Unternehmen und Privatanwender, mit denen die Welt etwas sicherer wird. Mit unseren Lösungen, die mit den Produkten anderer Unternehmen zusammenarbeiten, können Unternehmen Cyber-Umgebungen koordinieren, die wirklich integriert sind und in denen der Schutz vor sowie die Erkennung und Behebung von Bedrohungen nicht nur gleichzeitig, sondern auch gemeinsam erfolgen. McAfee bietet Schutz für alle Geräte von Privatanwendern und sichert dadurch das digitale Leben zu Hause und unterwegs. Durch die Zusammenarbeit mit anderen Sicherheitsakteuren fördert McAfee zudem den gemeinsamen Kampf gegen Cyber-Kriminelle. Davon profitieren alle.

www.mcafee.com/de

McAfee™
Together is power.

Ohmstr. 1
85716 Unterschleißheim
Deutschland
www.mcafee.com/de